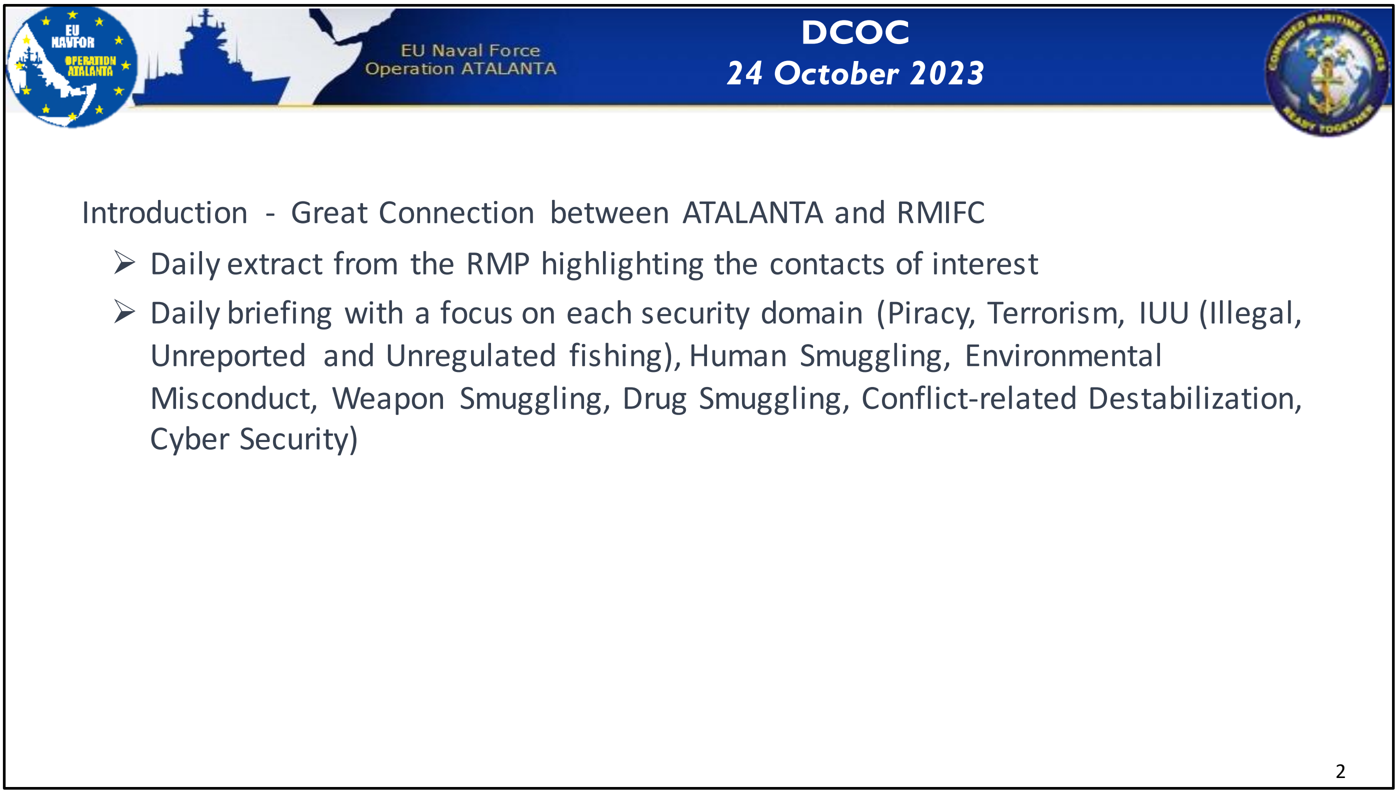
EU Naval Force
Operation ATALANTA

DCOC
24 October 2023

6th HIGH-LEVEL MEETING ON THE IMPLEMENTATION OF THE JEDDAH AMENDMENT TO THE DJIBOUTI CODE OF CONDUCT

CAPE TOWN – REPUBLIC OF SOUTH AFRICA
24-26 OCTOBER 2023

Utilizing the DCoC ISN to support operations at sea against illegal activities
Building on the MASE experience



EU Naval Force
Operation ATALANTA

DCOC
24 October 2023

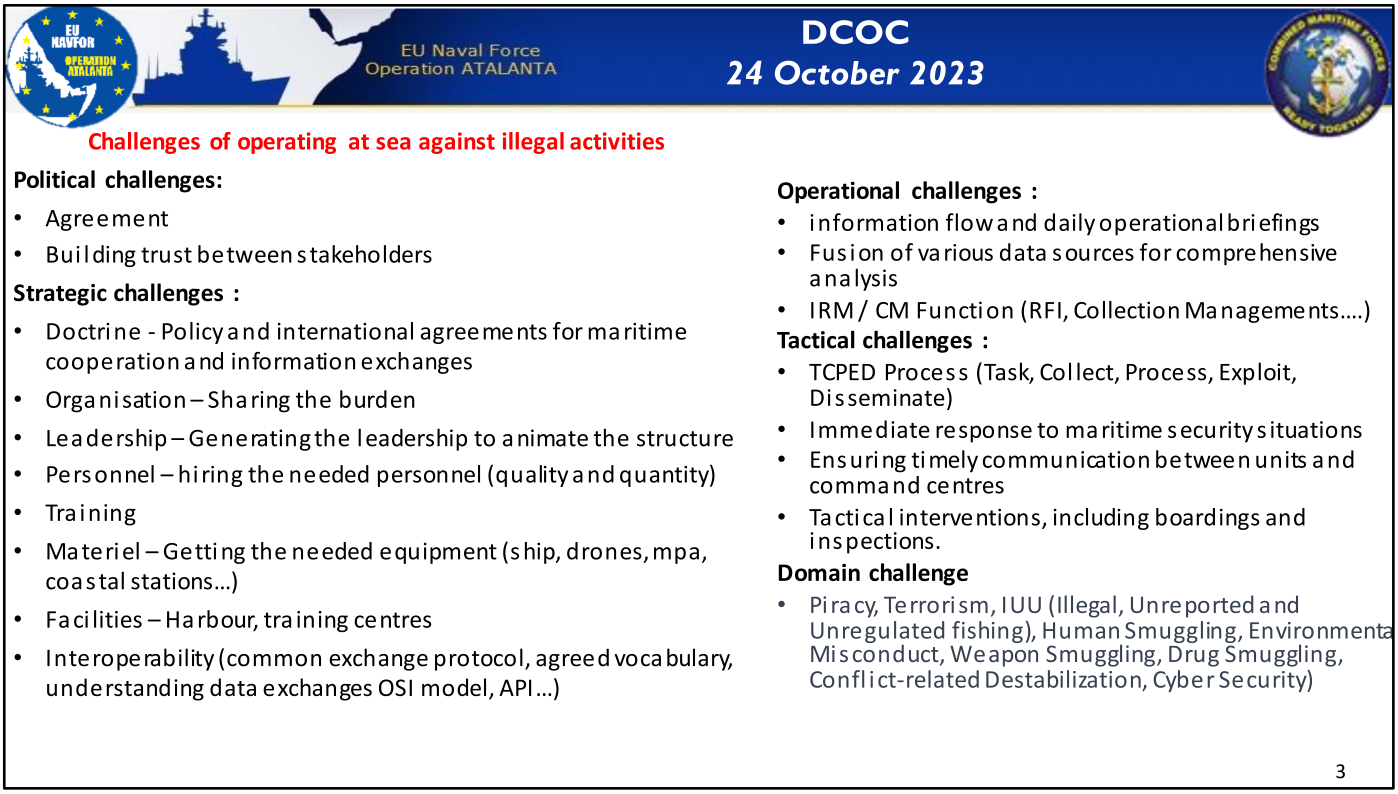
Introduction - Great Connection between ATALANTA and RMIFC

- ➢ Daily extract from the RMP highlighting the contacts of interest
- ➢ Daily briefing with a focus on each security domain (Piracy, Terrorism, IUU (Illegal, Unreported and Unregulated fishing), Human Smuggling, Environmental Misconduct, Weapon Smuggling, Drug Smuggling, Conflict-related Destabilization, Cyber Security)

2

Panel Discussion 2 – Utilizing the DCoC ISN to support operations at sea against illegal activities – Building on the MASE experience.

- We are receiving information daily from RMIFC Madagascar
- What they have done is impressive and very promising
- They share with us their daily Operational Briefing, which includes one slide for each Maritime Security Domain
- As you know, there are 7 maritime security domains which have been defined by M Ban Kee Moon in 2009 (Piracy, Terrorism, IUU, Human Smuggling, Environmental misconduct, Weapon smuggling, Drug Smuggling) and you shall add Conflict related destabilization and Cyber.
- Alone, you might have a small piece of the Puzzle but if you connect all the Information, and you work on the same power Point, toadd the information you have collected, at the end, you will have a decent presentation. Just need to agree on the template and the Workflow. Even better, if you can have a software which is already able to provide a layered approach to these domains, and you won't even need a ppt presentation.
- Today, we spend most of our time copying information from badly designed tool to PowerPoint in order to allow a better understanding of the situation. We tend to adapt to the tools instead of shaping the tools in accordance with our needs. You have the chance to have CRIMARIO willing to provide their expertise in the software development and related capacity building. Identify your needs and harass them until they provide what you expect.
- Challenges ahead:
  - The biggest challenge is **confidence**; after collection, sharing information is one of the biggest challenges in the intel domain. It requires trust and trust is not natural.
  - Its not only data protection, you might use encryption system, but also vetting: the question is 'who has access to the system ?'. If you know a highly valuable information, related to drug smuggling or weapons smuggling for instance, you don't want that information to be spoiled ; you want to be sure that all the people who may be behind the screen on which you are sharing this information need to know and are reliable. This is the most difficult to achieve. Until you reach that goal, you'll be limited in sharing unclassy non sensible information. but you can already share information on this kind of network. For instance, IUU related information may be shared on this kind of network
  - The secund challenge is **scarcity**. Most of the time, there is not much of interesting happening in the maritime domain. In the past months, the most common events were false alarms, captain threaten to encounter fishing skiff far away from the coasts, which proves that the piracy psychic trauma is still there. The maritime community needs to remain vigilant, of course, but also to be reassured. So, coming back to scarcity, there is not much to be done about it; you might have not much to report during several weeks and suddenly, putting together several information will allow to anticipate a maritime security breach ; but reporting that there is nothing significant happening is already an information.
  - The third challenge is **information rich but knowledge poor**. Having easily access to AIS information, LRIT information in some cases, provides thousands of tracks but doesn't tell much about the Maritime Security risk . this is where the automated analytic tools can provide an added value, budling correlation can eliminate the regular cases, or highlight the suspect cases. When you know the usual fishing area and you find a ship out of them pretending to fish, it might be worth a visit, at sea or when it reaches back a regional harbor, who knows what you might find… Pooling information from various sources is the key to identify those suspect cases.
  - The fourth challenge is **the tool** : the tool is always the limit. It will have an influence on what you can do and what you cannot do. It's like signal treatment, if you listen to a sound under the water, you might not find anything significant. But if instead of listening you display the sound on a frequency scale, which we call a Fourrier Transformation, you will immediately find if there is a submarine in the vicinity. In the maritime security domain, it's exactly the same, without a proper tool, you will just contemplate map full of information but with little knowledge.



EU Naval Force Operation ATALANTA

DCOC
24 October 2023

Challenges of operating at sea against illegal activities

Political challenges:

- Agreement
- Building trust between stakeholders

Strategic challenges :

- Doctrine - Policy and international agreements for maritime cooperation and information exchanges
- Organisation – Sharing the burden
- Leadership – Generating the leadership to animate the structure
- Personnel – hiring the needed personnel (quality and quantity)
- Training
- Materiel – Getting the needed equipment (ship, drones, mpa, coastal stations…)
- Facilities – Harbour, training centres
- Interoperability (common exchange protocol, agreed vocabulary, understanding data exchanges OSI model, API…)

Operational challenges :

- information flow and daily operational briefings
- Fusion of various data sources for comprehensive analysis
- IRM / CM Function (RFI, Collection Managements….)

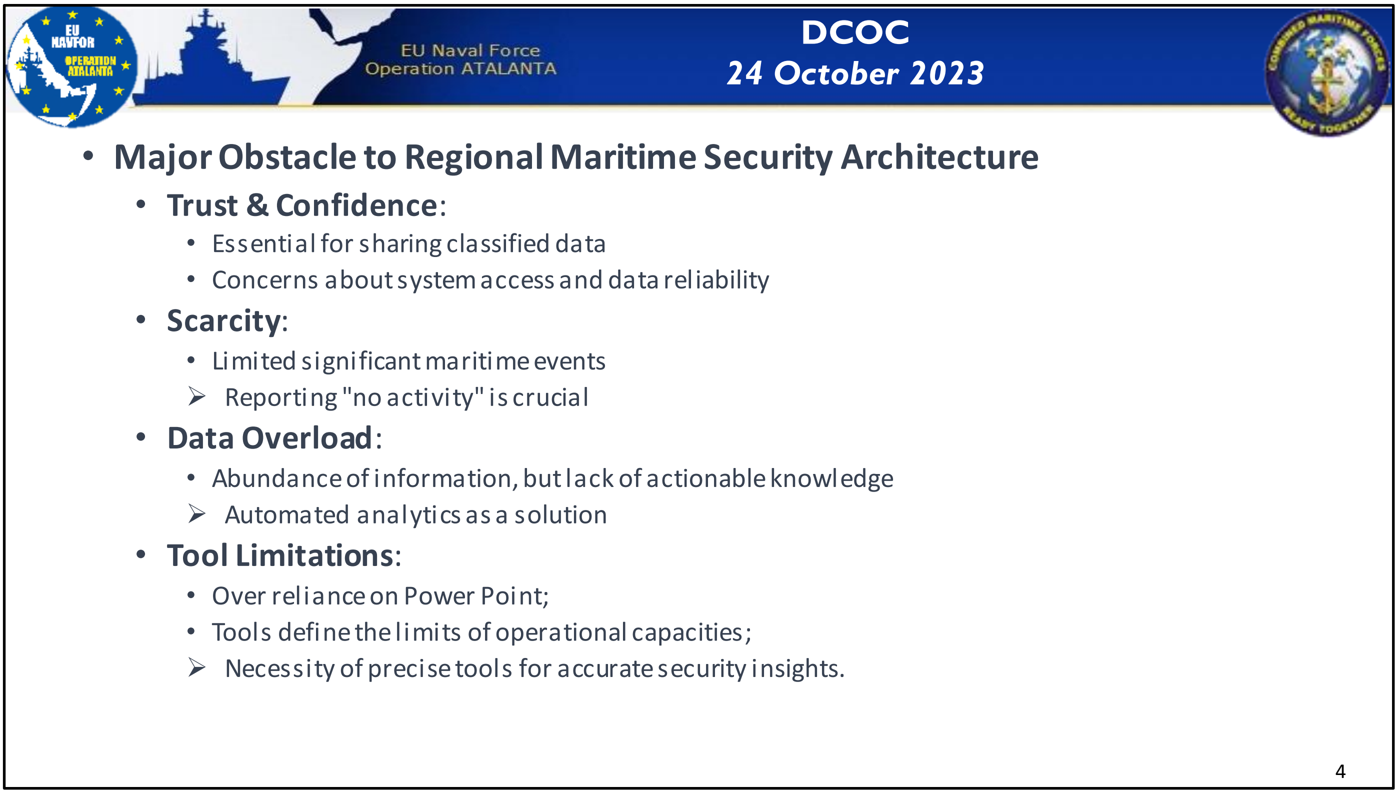
Tactical challenges :

- TCPED Process (Task, Collect, Process, Exploit, Disseminate)
- Immediate response to maritime security situations
- Ensuring timely communication between units and command centres
- Tactical interventions, including boardings and inspections.

Domain challenge

- Piracy, Terrorism, IUU (Illegal, Unreported and Unregulated fishing), Human Smuggling, Environmenta Misconduct, Weapon Smuggling, Drug Smuggling, Conflict-related Destabilization, Cyber Security)

DOTMLPF-I stands for:
- **D**octrine
- **O**rganization
- **T**raining
- **M**ateriel
- **L**eadership and Education
- **P**ersonnel
- **F**acilities
- **I**nteroperability



EU Naval Force
Operation ATALANTA

DCOC
24 October 2023

- **Major Obstacle to Regional Maritime Security Architecture**
  - **Trust & Confidence**:
    - Essential for sharing classified data
    - Concerns about system access and data reliability
  - **Scarcity**:
    - Limited significant maritime events
    - ➢ Reporting "no activity" is crucial
  - **Data Overload**:
    - Abundance of information, but lack of actionable knowledge
    - ➢ Automated analytics as a solution
  - **Tool Limitations**:
    - Over reliance on Power Point;
    - Tools define the limits of operational capacities;
    - ➢ Necessity of precise tools for accurate security insights.

4

EU Naval Force
Operation ATALANTA

DCOC

24 October 2023

End of presentation
Many thanks